How to mitigate "Weak XML Schema: Unbounded Occurrences" findings

This page has been made public for vendors

Question

How do I mitigate "Weak XML Schema: Unbounded Occurrences" findings? I cannot modify the schema.

Answer

This is a common concern since Fortify reports findings for all uses of "unbounded" for maxOccurs in a schema. Often application developers don't have control over the schema since it is for a third-party web service. Other times developers don't want to specify an upper bound due to concerns of poor performance from XML parsers when a large upper bound is specified.

These are legitimate concerns. However if the application is using the schema to parse incoming XML documents, using "unbounded" for maxOccurs puts the application at risk for a denial of service attack.

The solution (subject to verification during the A&A process and continuous monitoring as per VA Secure Code Review SOP) is to place limits on the XML file outside of the schema file:

- Some XML parsers provide configuration controls to limit the number of child elements that can be processed for each parent element. The developer should ensure any default values are appropriate for the application and are set to an appropriate value for mitigating a possible denial of service attack. For example, the Apache CXF Framework uses a parser that provides default limits.
- Limit the size of the incoming XML file that will be processed. Setting an upper bound for the document size effectively limits the number of elements that the XML document can hold. If one or more unbounded elements require extensive system resources, a denial of service scenario could still occur, however, this mitigation greatly reduces the risk.

The appropriate XML file size or the limit on the number of elements processed is application dependent. They should be set to appropriate values, low enough so that the application can successfully handle a denial of service scenario if the system is sent a large number of documents or elements within a document, yet high enough so legitimate documents are still accepted and processed.

Fortify will continue to report this finding, even if these mitigations are in place. Fortify cannot associate code that limits the XML file size, or a configuration control as the mitigation for unbounded occurrences in the schema. Developers must provide audit comments to describe the mitigations per the VA Secure Code Review SOP. For example, the developer should indicate the location in the code (file name, method or line numbers) where the limit on the size of the XML file is imposed, or link to documentation on the parser-imposed limits on the number of child elements.

References

- Weak XML Schema: Unbounded Occurrences - Fortify Taxonomy

HPE Fortify Version	4.42 and later
Programming Language	☐ C/C++ ☐ .NET ☐ Java ☐ Objective-C ☑ Other
Fortify Audit Workbench	☐ Yes ☑ No
Fortify IDE Plugin	☐ Yes ☑ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.